Chinese Hackers and Their New Target—Federal Employees

by: Ellen Cornelius, J.D.
Senior Law & Policy Analyst
The Center for Health & Homeland Security

Currently, the U.S. government monitors approximately 20 Chinese hacking groups; however, no system is flawless. Federal agencies reported that in fiscal year 2013, 9,883 malware attacks were launched.[1] The number of intrusions was not released.

In March 2014, Chinese hackers allegedly infiltrated the networks of the Office of Personnel Management (OPM), the Government Accountability Office (GAO), and the Government Printing Office (GPO).[2] Hackers gained access to the OPM database and installed malware on GAO servers; however, it is not clear how remotely the hackers maneuvered before they were stopped.[3]

It should be noted that tens of thousands of U.S. federal employees' personal information is stored on OPM servers. The GAO investigates and reports on how the federal government spends money. Among other duties, the GPO prints passports in response to applications received by the U.S. Department of State. OPM maintains files on employees who have applied for top-secret (TS) security clearances.[4] OPM, GAO, and GPO servers are attractive to hackers because they contain volumes of personnel systems upon which the aforementioned agencies rely, and in many cases, the information is of a highly confidential nature.

The nature of the hack is less important than the vulnerabilities that it exposed. If China launched a denial of service attack against the U.S. government, the result could be catastrophic. Denial of service attacks include sending requests that flood a network in an attempt to occupy network bandwidth or exploiting protocols to consume memory. Hackers are capable of causing more serious damage to infrastructure in the future.

Personally Identifiable Information

It is unclear how much information was exposed in the OPM, GAO, and GPO breaches, but the sheer number of federal employees makes these hacks deeply concerning. A Senior Department of Homeland Security Official stated that no personally identifiable information (PII) was compromised.[5] PII, for example, can be an individual's first and last name in combination with a Social Security Number, a Driver's License Number, a Financial Account Number, or an Individual Taxpayer Identification Number.[6] Federal employees and applicants utilize a program called e-Qip to enter data, including financial and personal information.[7] In turn, the federal government relies on the data in e-Qip to complete background checks. Accordingly, it is possible that a number of important data was compromised in the attack.

Although the private sector is required by state law to report data breaches to customers when there is a reasonable chance that the breach will result in data misuse, there was no such report by the federal government in this instance.[8] Other federal agencies, state governments, and local governments were notified about the intrusion, but given that the Obama Administration maintains that no PII was compromised, there was not a report.[9] While the private sector is held publicly accountable for their security breaches there is no such standard for the government leaving government employees to wonder about how much of their personal information may be compromised.

Chinese Hackers

Concerns about federal computer systems being hacked extend beyond data breaches. The U.S. government is constantly addressing threats from Chinese hackers. The Chinese military, or the People's Liberation Army (PLA), operates a large cyber command. Chinese technology analysts can participate in fighting wars by thwarting operational sustainment. Logistics, resupply, and personnel systems can be targeted virtually and result in physical losses.[10] In addition to kinetic attacks, the PLA's strategy includes electronic attacks.[11] For example, one of the PLA's goals is to prevent enemy commanders from communicating.[12] To achieve that aim, researchers at Shanghai Jiao Tong University's Department of Computer Science and Engineering reportedly developed a system that can generate and send 14 million network access requests, resulting in information attacks.[13] An information attack can be used to paralyze the enemy followed by a firepower attack.[14] In firepower attacks, civil infrastructure may be a target; political and economic entities may be important to the PLA in such a scenario.[15] Since *Unrestricted Warfare* was published in 1999, the PLA has set targets in cyber warfare strategy power systems, telecommunications systems, and educations systems.[16] Even if the firepower attacks do not destroy these systems, any disruption could tie up resources and divert attention, thereby having twin strategic and financial impacts.[17]

Identifying the perpetrators of cyberattacks is very difficult due to evolving technology that masks a hacker's identity.

Although the PLA engages in offensive and defensive technical operations, it also engages in psychological warfare, media warfare, and legal warfare.[18] The PLA attempts to affect public opinion in China by even simply being blamed for hacking into the U.S. government's databases. And perhaps even more importantly, if China successfully hacks into federal agencies' databases, then it can store the information from the government network until it is needed for exploitation, attack, or some other strategic value. Additionally, Chinese hackers may deposit malicious code, effective as critical intelligence, which will ease re-entry.[19]

U.S. Perspective

Chinese hackers can cause damage outside of traditional kinetic attacks. As such, the Obama Administration has taken a strong stance against state-run intelligence agencies using resources to obtain intellectual property for state-owned companies.[20] The Department of Justice (DOJ) released a most wanted list and included photographs of some of the alleged Chinese hackers.[21] In June 2014, DOJ indicted five members of PLA Unit 61398 for intellectual property theft.[22] Westinghouse Electric, United States Steel Corporation, United Steelworkers, and others were the subject of these cyberattacks.[23] DOJ's indictment alleges that members of PLA Unit 61398 hacked into Westinghouse's network, stole 700,000 pages of emails including some from the CEO, and learned Westinghouse's strategy for negotiating with a state-owned entity in China.[24] The indictment is largely a symbolic attempt to defend U.S. companies from Chinese attackers because it is extraordinarily unlikely, if not fantasy, that the Chinese government would extradite the indicted hackers. To date, the indictment and public shaming have not been successful. In fact, in the past two months, a different PLA unit attacked U.S. and European space and satellite technology companies and research groups.[25]

Identifying the perpetrators of cyberattacks is very difficult due to evolving technology that masks a hacker's identity. One senior U.S. official told the *New York Times* that the March 2014 attack could be definitively attributed to hackers in China.[26] Assuming that is true, it is not known whether the attack was carried out by Chinese government or by non-

government hackers. Some U.S. officials believe that the Chinese government participated in the attack because of the level of complexity and the subject matter.[27] Belief is insufficient for the purpose of U.S. policy. That is, unless attribution is definitive, the U.S. government does not have a policy that outlines responses to a large-scale attack on military or civilian networks.[28]

In addition to the complexities of attribution, the line between the Chinese government and the private sector is blurry. For example, Huawei is an independent Chinese technology company, which the U.S. government alleges is a shell corporation for the PLA.[29] U.S. government officials have broadcast their fear that Huawei would sell its equipment to the federal government or to the private sector, but create a "back door" in order to open the equipment's systems to military or government hackers in China.[30] There is evidence that the National Security Agency (NSA) hacked into the Huawei systems in order to intercept communications.[31] The NSA allegedly targeted Chinese leaders, Chinese military, and Ren Zhengfei, Huawei's founder.[32] In addition, the NSA may have manipulated Huawei's technology so it could monitor computer and telephone networks built on Huawei's equipment.[33]

"The IT sector in China can be considered a hybrid defense industry."[34] For example, Huawei operates in the commercial market yet benefits from a "background network of state research institutes and government funding in programs that do have affiliation or sponsorship of the PLA."[35] While Huawei publicly claims that it is not directly tied to the Chinese government, the fact that it receives funding from the PLA makes these claims baseless. Moreover, Huawei

develops tools that it markets to both the military and commercial sector.[36] This suggests a working relationship between Huawei's leaders, Chinese political leaders, and the PLA's leaders. The hybrid defense industry makes it difficult to identify hackers as state actors or non-state actors.

Conclusion

The OPM, GAO, and GPO hacks in March 2014 were high level breaches; moreover, they are indicative of the ever-deepening threat that Chinese hackers pose. Both the U.S. public sector and private sector need to increase their security measures in order to prevent similar attacks in the future. To this end, the National Institute of Standards and Technology (NIST) issued a voluntary framework for reducing cyber risks to critical infrastructure. Not only will the framework improve U.S. economic security, it may also benefit national security. Whether it will be a denial of service attack or something else, it is clear that Chinese hackers are able to launch attacks on the U.S. government's infrastructure. When they will do so remains the only unknown.

Ellen Cornelius received her J.D. from the University of Maryland in 2005 and is a member of the Maryland and District of Columbia bars. Since joining CHHS in 2008, Ms. Cornelius has worked for the District of Columbia's Homeland Security and Emergency Management Agency, the District's Business Emergency Management Operations Center, and served as a liaison to the Regional Catastrophic Preparedness Grant Program. Ms. Cornelius also co-teaches a course on the Law and Policy of Cybersecurity at the University of Maryland Francis King Carey School of Law.

CHHS
CENTER FOR HEALTH & HOMELAND SECURITY

1 Schmidt, Michael S. Chinese Hackers Extending Reach to Smaller U.S. Agencies, Officials Say. New York Times. July 15, 2014.
2 Id.
3 Id.
4 Id.
5 Schmidt, Michael S. Sanger, David E., Perlroth, Nicole. Chinese Hackers Pursue Key Data on U.S. Workers. New York Times. July 9, 2014.
6 Maryland Personal Information Protection Act. Md. Code Annotated Commercial Law 14-3504. 2008.
7 Id.
8 Id.
9 Id.
10 Wortzel, Larry M. The Chinese People's Liberation Army and Information Warfare. Strategic Studies Institute and U.S. Army War College Press. March 2014. Page 15.
11 Id. at 10.
12 Id. at 15.
13 Krekel, Bryan. Adams, Patton. Bakos, George. Occupying the Information High Ground: Chinese Capabilities for Computer Network Operations and Cyber Espionage. U.S.-China Economic and Security Review Commission by Northrup Grumman Corp. March 7, 2012. Page 33.
14 Wortzel, Larry M. The Chinese People's Liberation Army and Information Warfare. Strategic Studies Institute and U.S. Army War College Press. March 2014. Page16.
15 Id. at 11.
16 Id. at 16.
17 Id. at 14.
18 Id. at vii.
19 Id. at 19.
20 Schmidt, Michael S. Sanger, David E. 5 in China Army Face U.S. Charges of Cyberattacks. New York Times. May 19, 2014.
21 Id.
22 Schmidt, Michael S. Sanger, David E., Perlroth, Nicole. Chinese Hackers Pursue Key Data on U.S. Workers. New York Times. July 9, 2014.
23 Schmidt, Michael S. Sanger, David E. 5 in China Army Face U.S. Charges of Cyberattacks. New York Times. May 19, 2014.
24 Id.
25 Schmidt, Michael S. Sanger, David E., Perlroth, Nicole. Chinese Hackers Pursue Key Data on U.S. Workers. New York Times. July 9, 2014.
26 Id.
27 Id.
28 Krekel, Bryan. Adams, Patton. Bakos, George. Occupying the Information High Ground: Chinese Capabilities for Computer Network Operations and Cyber Espionage. U.S.-China Economic and Security Review Commission by Northrup Grumman Corp. March 7, 2012. Page 32.
29 Sanger, David E. Perlroth, Nicole. N.S.A. Breached Chinese Servers Seen as Security Threat. New York Times. March 22, 2014.
30 Id.
31 Schmidt, Michael S. Sanger, David E., Perlroth, Nicole. Chinese Hackers Pursue Key Data on U.S. Workers. New York Times. July 9, 2014.
32 Id.
33 Sanger, David E. Perlroth, Nicole. N.S.A. Breached Chinese Servers Seen as Security Threat. New York Times. March 22, 2014.
34 Krekel, Bryan. Adams, Patton. Bakos, George. Occupying the Information High Ground: Chinese Capabilities for Computer Network Operations and Cyber Espionage. U.S.-China Economic and Security Review Commission by Northrup Grumman Corp. March 7, 2012. Page 68.
35 Id.
36 Id. at 75.